Remember To Look Next To You When Eliminating IA Threats

August 2008

Do you sleep well at night knowing your house and everything in it is safe? Have you installed the best door locks, burglar alarms and motion sensitive lights available? Is Spot, your Doberman/pit bull/wolf family pet awake, alert and a little hungry? Does your exterior resemble a bunker with siding that could withstand a force five hurricane? Then what's that sound of something destroying your home? A possible answer; termites, the threat from within. Your mission critical data could be at as much risk.

The cyber fences that protect the Army's data and communications are state of the art and improving. They include the best available tools, such as firewall and virus scanners, supported by proven best business practices with dedicated professionals poised to identify and react to threats. Yet a large percentage of malicious network attacks and incidents of data compromise does not come from terrorist organizations, rogue states, organized crime or even a mischievous teenager. It comes from within the organization.

Before you start thinking that Bob in the next cube or Jane down the hall is after your data, realize that internal threats come from two main sources: the unhappy and the untrained. The unhappy, or potentially unhappy, are easier to spot. Anyone who is preparing to leave, has just been let go, chewed out by the boss, or humiliated by coworkers can become an insider threat. For example, a private first class at an Army's major personnel records center had been recently punished for various conduct/performance issues. For revenge, he installed unauthorized remote administration software so he could access the network from home. After gaining access, he deleted 58,000 personnel records.

However, people that lack training or attempting to skirt the rules just to set things up "their way" are as much of a threat. Another example is the case of a watch officer working night shifts in a sensitive facility. To pass the time and fight boredom, the watch officer tried to install personal gaming software, but his account permissions prevented it. He then installed a key logger on a classified system in order to capture the administrator's login credentials. This allowed him access to the classified system to install the game. It was fortunate that was all he wanted to do.

The number of people who have caused problems because they didn't know what they were doing could fill a few books. I remember my own introduction to this potential threat when a temporary worker went to format a new data disk (Yeah, it's an old story) and reformatted the hard drive erasing five critical databases. Back then, it was a lot harder to recover and we won't even get into the backup issues.

Here are some general suggestions for helping to prevent internal threats to data integrity.

- Establish and enforce out-processing policies that include identifying and terminating network accounts. Don't forget about AKO and other remotely offered services.
- Immediately delete the account of someone who as moved on for any reason. This prevents the creation of orphan accounts or accounts that have no owner because the original owner either left the organization or the project.
- Be aware of and on guard for potential internal threats from someone that displays signs of not being fully "gruntled."
- Install and maintain the internal forensic tools necessary to track and prevent internal threats.
- Ensure that all personnel are fully and appropriately trained to avoid errors in judgment or actions that could result in data loss or compromise.

- Keep in mind that free downloads of software are prohibited, and often accompanied by malicious software that poses a substantial risk to the user and the network.
- Inspect and review audit and system logs periodically for signs of suspicious behavior.

The main lesson is not only to protect your data's home with strong walls and locked doors, but check for termites as well.